Title	Digital Forensics
Long Title	Digital Forensics
Credits	**10**
NFQ Level	Expert
Module Author	Prof Donna O'Shea

Module Description:

In this module students will learn how to identify, collect and preserve digital evidence on different operating systems. They will develop skills to analyze both static and volatile data, required as part of a forensic investigation and how to write a report that can be later used as evidence in court.

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1	Set up a forensic workstation with the aim of collecting and preserving digital evidence.
LO2	Gather and analyze static data from a computer or storage device with the aim of preserving digital evidence.
LO3	Acquire and analyze volatile memory and data using tools and data forensics techniques.
LO4	Conduct forensic analysis in multiple operating systems and environments.
LO5	Write a forensic report complying to international best practice and law.
LO6	Analyse the main anti forensic techniques and their impact in conducting a forensic investigation

Indicative Content

Computer Forensics

What is it, why is it important. Types of computer forensics – networks, email, malware, memory, mobile phones, database and disk. Techniques used by cyber forensics investigators – reverse steganography, stochastic forensics, live analysis, file recovery etc. Process used by forensic investigators – acquire, identify, evaluation and admission etc.Setting up forensic workstation. Deployable cyber evidence collection i.e. deployable forensics.

Operating Systems & File Systems

Fundamentals of file systems – Windows, Linux, Mac. Windows FAT and NTFS. SSD versus HDD. Microsoft windows registry. Linux Extended File System (Ext4). MAC Hierarchical File System (HFS), and Extended Format File System (HFS+). Tools - Sleuth Kit, Autopsy tools, ProDiscover, WinHex,
WindowsScope OSForensics, FTK Imager, RootKit revealer.

Acquiring non-volative memory (static acquisition)

Sources of memory: RAM, hyberfil, swap/page file. Evidential artifacts in memory. Acquisition tools and standard operating procedures. String searching and pattern recognition. Memory analysis - tools and techniques. Ethical considerations.

Acquiring volatile memory (live acquisition)

Acquiring volatile memory. The live data forensics process. Volatile data categories and sources i.e.network data. Search techniques, tools and tool kit preparation. Tools and standard operating procedures. Volatile data acquisition, analysis and reporting.

Forensic Analysis

Data Carving, Timeline Analysis, supertimelines, unallocated data, slack space, Host Block Area, Windows Registry Keys, restore points, ShellBags,Finding evidence of file opening/download/execution, physical location, external device usage, browser usage, account login/logout.

Anti Forensic Techniques

Encryption. Program packers. Overwriting data. Onion Routing. Steganography. Changing timestamps.

Writing Reports

Importance of writing reports. Preparing reports complying with country laws. Writing reports guidelines. Extracting data from software for reporting.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Project	Given log file data the student may be expected to gather static and volatile data using well known tools and techniques with the aim of perserving evidence that may form part of an forensic investigation. They will write a report as part of their findings.	1,2,3,4,5	70.0	Week 9
Project	This project will evaluate the students understanding on the main anti forensics techniques and their impact on a forensic investigation and analysis.	1,2,3,4,5,6	30.0	Sem End

No End of Module Formal Examination

Assessment Breakdown	**%**
Coursework	100

Re-Assessment Requirement

Coursework

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes	3.0	Every Week	3.0
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.0

Independent & Directed Learning (Non-contact)	Independent learning by the student.	9.0	Every Week	9.0
		Total Hours		14
		Total Weekly Learner Workload		14
		Total Weekly Contact Hours		5

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes.	3.0	Every Week	3.0
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	9.0	Every Week	9.0
		Total Hours		14
		Total Weekly Learner Workload		14
		Total Weekly Contact Hours		5

Recommended Book Resources

- **Jason Luttgens, Matthew Pepe, Kevin Mandia 2014, Incident Response and Computer Forensics [ISBN: 9780071798686]**